IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Volume-6, Special Issue-2, March 2018 E-ISSN: 2347-2693

An Efficient Cloud Storage Based On Key Aggregate Searchable Encryption for Group Data Sharing

Paramasivam[1], L.Jayasimman[2*], R.Saradha[3]

[1]Department of Computer Science, Srimad Andavan Arts and Science College (Autonomous), Trichy-620005
[2]Department of Computer Science, Srimad Andavan Arts and Science College (Autonomous), Trichy-620005
[3] Department of Computer Science, Srimad Andavan Arts and Science College (Autonomous), Trichy-620005

Available online at: www.ijcseonline.org

Abstract Broadcasting the encrypted data via cloud storage may greatly ease security concerns.. Security is provided to access data in wireless broadcast services. Symmetric-key-based encryption is used to ensure the authorized users who own the valid keys can decrypt the data. With regard to various subscription activities, an efficient key management for distributing and changing keys is in great demand for the access control in broadcast services. Hence the proposed system namely, key tree reuse (KTR) to handle key distribution with regard to complex subscription options and user activities. It contributes all subscription activities in wireless broadcast services. Instead of separate sets of keys for each program, a user only needs to hold one set of keys for all subscribed programs. KTR identifies the minimum set of keys that must be altered to ensure broadcast security and minimize the rekey cost.

Keywords: Searchable encryption, data sharing, data privacy.

I. INTRODUCTION

Cloud computing is the result of the progression and implementation of existing technologies ensuring the effective secure environment for users. The objective of cloud computing is to allow users to take benefit from all of these technologies, without the need for deep acquaintance about with each one of them. The cloud aims to decrease the quite a not many costs, and help the users focus on their core business instead of being impeded by IT obstacles. The important technology used in the cloud computing is virtualization. Virtualization software separates a bodily compute machine into one or additional "virtual" devices, each of which can be easily used and managed to perform computing tasks. With operating system–level virtualization fundamentally creating a scalable system of multiple independent computing devices, idle computing resources can be allocated and used more efficiently. Virtualization provides the nimbleness essential to speed up IT operation, and reduce cost by increasing infrastructure utilization. This type of computing automates the process from end to end which the user can condition resources on-demand. By reducing user involvement, automation speeds up the progression, lower labor costs and reduces the occasion of human errors. Users consistently face difficult business problems in several manipulation processes. Cloud computing adopts concepts and function from many resources such as Service-oriented Architecture that may help the user to smash these problems into services that can be incorporated to provide a solution. Cloud computing provide all of its income as military, and make employ of the entrenched principles and best practices gained in the domain of SOA to allow global and easy access to cloud services in a regular way.

Broadcasting is the portion of signal which transmits programs to the spectators. The spectators might be the general community or a relatively large sub-audience. The process of sequencing of content in a broadcast is called a schedule. Television and radio programs are widely distributed through radio broadcasting or cable, often both simultaneously. By coding signals and having decoding equipment in homes, the later also enables subscription-based channels and pay-per-view services. Broadcast originally referred to the sowing of seeds by spreading them over a wide field. It was adopted by early radio engineers from the Midwestern United States to refer to the analogous dissemination of radio signals. Broadcasting forms a very large sector of the mass media. Process of Broadcasting to a very slight range of listeners is called narrowcasting.

Distribution in communication is widely used in the world of broadcasting. There are many forms of broadcast, but they all aim to distribute a signal that will reach the target viewers. Broadcasting can arrange listeners into entire assemblies. Many businesses take merits of communication dissemination in advertising over broadcasts. The options are close to limitless with advancing technology. The major goal is simply obtain the message across and it is up to the consumer inhabitants and listeners to do what they wish with it. In computer networking, broadcasting is a procedure of transmitting a package that will be conventional (conceptually) by each machine on the network like hub. In practice, the scope of the broadcast is restricted to a broadcast domain. With the ever-growing reputation of smart mobile devices, along with the rapid advent of wireless technology, there has been an increasing concern in wireless data services among both industrial and studious communities in recent years. Among various approaches, broadcast allows a very efficient usage of the scarce wireless bandwidth, because it allows parallel access by an arbitrary number of mobile clients. In a Wireless networks, broadcast services have been available as commercial products for many years. In particular, the announcement of the MSN Direct Service (www.direct.msn.com) has further highlighted the business interest in and the achievability of utilizing broadcast for wireless data services.

II. RELATED WORK

Multi-user Searchable Encryption

There is a prosperous literature on searchable encryption, together with SSE schemes and PEKS schemes. In contrast to those existing effort, in the perspective of cloud storage, keyword search below the multi-tenancy setting is a more common scenario. In , the data owner would like to share a document with a group of authorized users, and each user who has the access right can give a trapdoor to perform the keyword search over the shared document, namely, the "multi-user searchable encryption" (MUSE) scenario. Some recent work focus to such a MUSE circumstances, although they all adopt single-key combined with access control to attain the goal. In MUSE schemes are constructed by allocating the document's searchable encryption key with authorized users who can access it, and broadcast encryption is used to obtain coarse-grained access control. In attribute based encryption (ABE) is used to achieve fine-grained access control awake keyword search. As an effect, in MUSE, the main difficulty is how to control which users can access which documents, whereas how to reduce the number of shared keys and trapdoors is not considered. Key collective searchable encryption can give the solution and it can create MUSE more efficient and practical.

Group data sharing system based Evaluation

To advance the existing system, the caching based improved technique need to be used to perform more effective way of keyword searching. In a Processing, when an aggregate single trapdoor is received and the cloud server executes the KASE. Considering the time assessment cost of Adjust algorithm is linear when plotted against the number document

III. METHODOLOGY

PROPOSED SYSTEM

To proposition the original conception of key-aggregate searchable encryption (KASE) explaining the notion through a concrete KASE system.

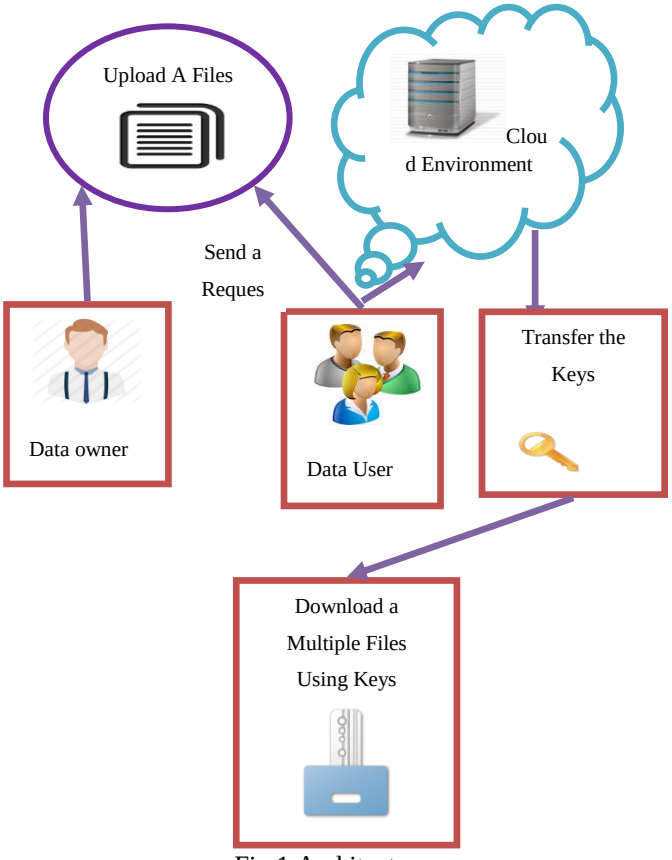


Fig 1.Architecture

The fig.2 shows the efficient architecture to approach the Key-aggregate searchable encryption (KASE) with different set of modules.

Data owner share the files on cloud storage provides secure cloud environment. To access the file, the authorized user requests the data owner and gets the encrypted unique key to acquire the required file.

The proposed KASE scheme applies to any cloud storage that supports the searchable group data sharing functionality, which means any user may selectively share a group of selected files with a group of selected users, while allowing the latter to perform keyword search over the former. First define a general framework of key aggregate searchable encryption (KASE) composed of seven polynomial algorithms for security parameter setup, key generation, encryption, key extraction, trapdoor generation, trapdoor adjustment, and trapdoor testing

PROCESS FLOW:

1. Setup Phase (DATA USER)
2. Encrypt Phase
3. Key Gen Phase,
4. Key Aggregator
5. Decrypt Phase
6. Digital signature

3.1 SETUP PHASE (data user)

The setup algorithm takes no contribution other than the implicit safety parameter. It outputs the community parameters PK and a master key MK.

3.2 ENCRYPT PHASE

Encrypt (PK, M, A). The encryption algorithm takes as input the public parameters PK, a message M, and an admittance structure A above the creation of attributes

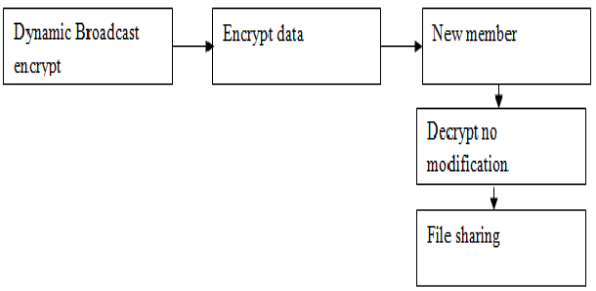


Fig 2. Encrypt Phase

The algorithm will encrypt M and build a cipher text CT such that simply a user that possesses a set of attribute that satisfies the access arrangement will be able to decrypt the significance. We will suppose that the cipher text implicitly contains A. the Fig2 shows the procedure of encrypt phase and give the secure surroundings to admission the required file.

3.3 KEY GEN PHASE

The input generation algorithm takes as input the master key MK and a put of attributes S that explain the key. It outputs a private key SK

3.4 KEY AGGREGATOR

The data owner establish the public system parameter via Setup and generate a public/master-secret3 key pair via Key Gen. Messages can be encrypted via Encrypt by anyone who also decide what cipher text class is connected with the plaintext significance to be encrypted. The data proprietor can use the master-secret to generate an collective decryption key for a set of cipher text classes via Extract. The generated keys can be passed to delegate securely (via secure e-mails or secure devices) lastly; any user with an aggregate input can decrypt some cipher text provided that the cipher text's class is restricted in the aggregate key via Decrypt4.

3.5 DECRYPT PHASE

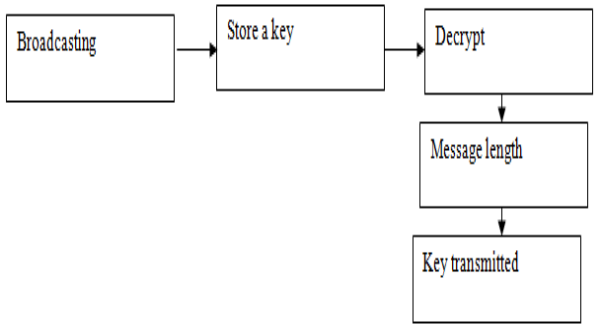


Fig 3.Decrypt Phase

Decrypt (PK, CT, and SK). The decryption algorithm obtain as donation the society parameters PK, a cipher text CT, which contain an access policy, a and a private key SK, which is a private key for a position S of attributes. If the set S of attributes satisfies the admittance structure A then the

algorithm will decrypt the cipher text and go back a message M.

3.6 DIGITAL SIGNATURES

A digital mark (not to be confused with a digital certificate) is a numerical process used to authenticate the authenticity and honesty of a message, software or digital document. Digital signatures can provide the additional assurance of proof to origin, individuality and status of an electronic document, business or message, as well as acknowledging informed consent by the signer.

ENHANCED IDENTITY BASED ENCRYPTION ALGORITHM

1. Alice authenticates with the SKG and receives her confidential solution EIDAlice.

2. Using her confidential key EIDAlice, Alice generate σ for M and pass it to Bob, possibly along with encrypted implication C over.

3. After getting M and σ from Alice, Bob checks whether σ is an authentic signature on M using Alice's individuality ID and the SKG's public key skSKG.

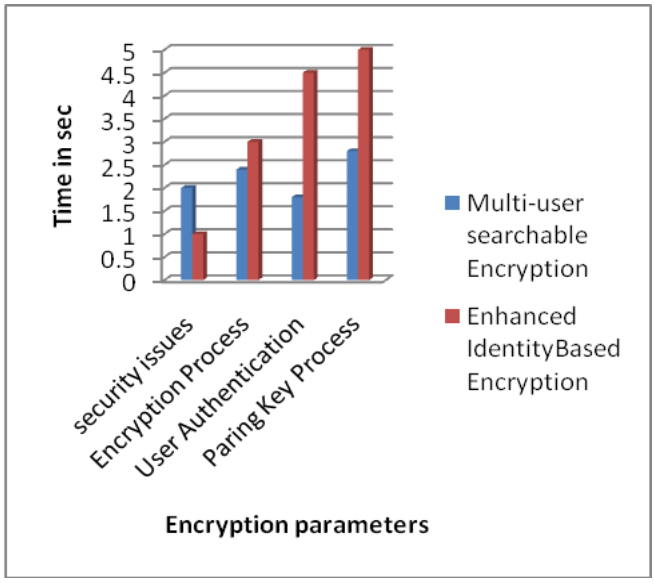
4. If above conditions satisfy it proceeds "Accept". Otherwise, returns "Reject". Note that Bob doesn't need to have some type record for Alice.

Enhanced Identity-based systems allow user to generate a public key from a known identity charge such as an ASCII string. A trusted authorized third party, called the secure key generator (SKG), generates the consequent private keys. To activate the SKG first publish a master public enter, and retain the equivalent master private key (referred to as master key). Given the master public key, any party can compute a public key equivalent to the identity ID by combining the master public key with the individuality value. To obtain a matching private input, the party certified to use the identity ID contacts the SKG, which uses the master private key to generate the private key for identity ID. Enhanced Identity-based systems allow any gathering to produce a public key from a known identity price such as an ASCII string.

To drive the SKG first publishes a master public key and retains the corresponding master private key (referred to as master key). Set the master public key for further manipulation. So that any gathering can compute a public key equivalent to the identity ID by combine the master public enter with the identity value. To attain a corresponding private key, the party authorized to use the identity ID contacts the SKG, which uses the master private key to generate the private key for identity ID for the further process.

As a result, users may encrypt messages (or verify signatures) with no prior distribution of keys between individual participants. This is enormously helpful in cases where pre-distribution of authenticated keys is inconvenient or infeasible due to technical restraints. However, to decrypt or warning messages, the official user must get the suitable confidential key from the SKG. A vigilance of this approach is that the SKG must be highly trusted, as it is able of generating any user's private key and may therefore decrypt (or sign) messages without permission.

PERFORMANCE ANALYSIS



Graph1. Performance analysis

From the above Graph1, the proposed concept of key-aggregate searchable encryption (KASE provide an effective result to building realistic data sharing system based on public cloud storage than existing algorithm in the field of Security, Encryption and Allocation of unique key to authorized users.

IV. CONCLUSION

Searchable encryption is a momentous cryptographic primordial that is glowing aggravated by the

reputation of cloud storage services like Drop box, Microsoft Sky Drive and Apple iCloud and public cloud storage infrastructures like Amazon S3 and Microsoft Azure Storage. Any practical SSE scheme, however, should convince certain properties such as sub linear (and preferably optimal) search, adaptive security, compactness and the ability to support addition and deletion of files.

REFERENCE

[1] S. Yu, C. Wang, K. Ren, and W. Lou, "Achieving Secure, Scalable, and Fine-Grained Data Access Control in Cloud Computing", Proc. IEEE INFOCOM, pp. 534-542, 2010.

[2] R. Lu, X. Lin, X. Liang, and X. Shen, "Secure Provenance: The Essential of Bread and Butter of Data Forensics in Cloud Computing", Proc. ACM Symp. Information, Computer and Comm. Security, pp. 282-292, 2010.

[3] X. Liu, Y. Zhang, B. Wang, and J. Yan. "Mona: secure multiowner data sharing for dynamic groups in the cloud", IEEE Transactions on Parallel and Distributed Systems, 2013, 24(6): 1182- 1191.

[4] C. Chu, S. Chow,W. Tzeng, et al. "Key-Aggregate Cryptosystem for Scalable Data Sharing in Cloud Storage", IEEE Transactions on Parallel and Distributed Systems, 2014, 25(2): 468-477.

[5] X. Song, D.Wagner, A. Perrig. "Practical techniques for searches on encrypted data", IEEE Symposium on Security and Privacy, IEEE Press, pp. 44C55, 2000.

[6] R. Curtmola, J. Garay, S. Kamara, R. Ostrovsky. "Searchable symmetric encryption: improved definitions and efficient constructions", In: Proceedings of the 13th ACM conference on Computer and Communications Security, ACM Press, pp. 79-88, 2006.

[7] P. Van,S. Sedghi, JM. Doumen. "Computationally efficient searchable symmetric encryption", Secure Data Management, pp. 87-100, 2010.

[8] S. Kamara, C. Papamanthou, T. Roeder. "Dynamic searchable symmetric encryption", Proceedings of the 2012 ACM conference on Computer and communications security (CCS), ACM, pp. 965-976, 2012.

[9] D. Boneh, C. G, R. Ostrovsky, G. Persiano. "Public Key Encryption with Keyword Search", EUROCRYPT 2004, pp. 506C522, 2004.

[10] Y. Hwang, P. Lee. "Public Key Encryption with Conjunctive Keyword Search and Its Extension to a Multi-user System", In: Pairing-Based Cryptography C Pairing 2007, LNCS, pp. 2-22, 2007.

